■ ธีรา ทานตวณิช

ปัจจุบันการค้าผ่านอินเทอร์เน็ตหรือ ECommerce กำลังได้รับความสนใจเป็นอย่างมาก หลายคนเริ่มศึกษาและหาช่องทางธุรกิจเพื่อนำมาเปิดบริการ อีกหลายคนเริ่มคิดจะพัฒนาหน้าเว็บไซท์สำหรับร้านค้าของตน แต่สิ่งหนึ่งที่จำเป็นที่ผู้จะดำเนินธุรกิจโดยการเปิดเว็บขายของต้องคำนึงถึงคือ ความปลอดภัยของข้อมูล

เป็นที่รู้กันทั่วไปว่าการค้าบนอินเทอร์เน็ตจะต้องอำนวยความสะดวกให้ผู้ซื้อสามารถสั่งซื้อแบบอัตโนมัติได้ด้วย จึงจะได้เปรียบ โดยผู้ซื้อจะต้องใส่ชื่อ รายละเอียดบัตรเครดิต ที่อยู่ และข้อมูลส่วนตัวที่เป็นความลับอื่น ๆ ลงบนหน้าเว็บของท่าน ดังนั้นผู้ขายจะต้องมีระบบรักษาความปลอดภัย เพื่อเป็นการให้ความมั่นใจกับลูกค้าว่า ข้อมูลต่าง ๆ เหล่านั้นได้รับการปกป้องจากการลักลอบดักเอาข้อมูลไปใช้ในทางที่ผิด

# Web Security : ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce

*ระบบรักษาความปลอดภัยสำหรับการทำ E-Commerce วิธีหนึ่งที่มีประสิทธิภาพ*

บทความนี้จะเสนอวิธีการจัดระบบรักษาความปลอดภัยสำหรับการทำ E-Commerce วิธีหนึ่ง นั่นคือการรักษาความปลอดภัยข้อมูลที่ถูกส่งผ่านหน้าเว็บจากฝั่งลูกค้าที่กรอกลงบน Web Browser และส่งมายังเครื่อง Server ซึ่งเราเรียกว่า Web Security

Web Security เป็นการรักษาความปลอดภัยสำหรับข้อมูลบนหน้าเว็บ ซึ่งปัจจุบันมีการพัฒนารูปแบบ Web Security นี้หลายรูปแบบ โดยใช้โปรโตคอลสำหรับความปลอดภัยต่าง ๆ กัน ผู้เขียนขอยกมา 3 โปรโตคอลว่าแต่ละอย่างทำงานอย่างไร และจะนำมาประยุกต์เข้ากับระบบของท่านได้อย่างไร เริ่มกันเลยดีกว่าค่ะ

## SSL : Secure Sockets Layer Protocol

โปรโตคอล SSL นี้ถูกพัฒนาขึ้นโดย Netscape Communications โดยมีวัตถุประสงค์หลักคือ การจัดระบบรักษาความปลอดภัย โดย SSL จะจัดช่องทางหรือ Session ที่ปลอดภัยสำหรับการติดต่อส่งข้อมูล โดยในปัจจุบัน SSL ถูกนำไปพัฒนาและมีการใช้งานในหลายรูปแบบ ซึ่งรูปแบบส่วนใหญ่จะเป็นการติดต่อส่งข้อมูลระหว่างเครื่อง Web Server กับโปรแกรม Browser เพื่อการติดต่อส่งข้อมูลทาง World Wide Web ให้ปลอดภัยมากขึ้น ซึ่ง SSL ได้รับความนิยมในการนำมาเป็นส่วนรักษาความปลอดภัยในการติดต่อระหว่างผู้ขายกับผู้ซื้อในงาน E-Commerce โดยจะเห็นได้จาก Web Browser และซอฟต์แวร์สำหรับทำ Web Server ทุกยี่ห้อรองรับการทำงานของโปรโตคอล SSL ทั้งนั้น

# Web Security : ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce

โปรโตคอล SSL ทำงานอยู่เหนือชั้น Transport หรือชั้นที่ 4 ใน OSI Model ซึ่งจะคอยจัดช่องทางที่ปลอดภัยระหว่างชั้น Transport กับแอพพลิเคชันที่อยู่เหนือขึ้นไป

โดยปกติเครื่องคอมพิวเตอร์ 2 เครื่องจะติดต่อกันข้ามเครือข่ายผ่านทางช่องทางหรือ Socket ที่กำหนดกันไว้ล่วงหน้า เช่น Web Browser ของผู้ใช้งานจะติดต่อไปยัง Web Server ที่เก็บเว็บไซท์ที่ผู้ใช้งานเรียกไป โดยใช้โปรโตคอล HTTP ทางพอร์ต 80 แต่ SSL จะจัดพอร์ตการติดต่อที่ต่างออกไปจากพอร์ตธรรมดานี้ คือจะให้ติดต่อกันที่พอร์ต 443 แทน ดังนั้น SSL จึงสามารถนำไปใช้งานกับโปรโตคอลในชั้นแอพพลิเคชันอื่น ๆ ได้ เช่น FTP, TELNET, gopher, NNTP และ SMTP

ใน SSL เครื่อง 2 เครื่องจะตกลงเพื่อร่วมกันสร้างกุญแจสำหรับช่องทางการติดต่อแต่ละครั้งโดยเฉพาะ ซึ่งจะเรียกขั้นตอนนี้ว่า การทำ Handshake เริ่มจาก Client (ในกรณีนี้เป็น Web Browser) ร้องขอเปิดการติดต่อไปยัง Server โดยจะระบุหมายเลขประจำการติดต่อ อัลกอริธึมสำหรับการเข้ารหัส และวิธีการบีบอัดข้อมูลสำหรับการติดต่อครั้งนั้น ซึ่ง Server จะตอบกลับยืนยันกุญแจสาธารณะส่วนเซิร์ฟเวอร์ อัลกอริธึม และวิธีการบีบอัดข้อมูล รวมทั้งเซิร์ฟเวอร์จะส่งหนังสือรับรองว่าเซิร์ฟเวอร์ที่ไคลเอนต์กำลังติดต่ออยู่นี้เป็นตัวตนจริง ๆ กับที่ไคลเอนต์ต้องการติดต่อด้วย

ไคลเอนต์ตรวจสอบหนังสือรับรองแล้ว ก็จะเอากุญแจสาธารณะที่ได้รับมาเข้ารหัสด้วยกุญแจที่ไคลเอนต์สร้างขึ้นมาเอง สิ่งที่ได้ก็คือกุญแจสำหรับการติดต่อในครั้งนั้น หรือ Session Key ซึ่งไคลเอนต์จะส่งให้เซิร์ฟเวอร์เพื่อให้ทั้ง 2 ฝ่ายใช้ Session Key เข้ารหัสในการติดต่อครั้งนั้น ๆ (ในขณะเดียวกันหากเซิร์ฟเวอร์ต้องการขอตรวจสอบหนังสือรับรองของไคลเอนต์ ก็จะส่งไปให้เซิร์ฟเวอร์พร้อม ๆ กันนี้เลย)

จะเห็นได้ว่าเซิร์ฟเวอร์จะต้องมีใบรับรองที่ออกโดยองค์กรผู้ออกใบรับรอง หรือ Certificate Authority (CA) ดังนั้นหากท่านต้องการสร้างเว็บไซท์สำหรับขายสินค้าแบบ E-Commerce และต้องการติดตั้งเครื่องเซิร์ฟเวอร์สำหรับร้านค้า E-Commerce ของท่านเอง ท่านจะต้องปฏิบัติตามขั้นตอนต่าง ๆ เพื่อให้เว็บไซท์ของท่านมี SSL รักษาความปลอดภัย ซึ่งผู้เขียนอยากจะขอแนะนำเป็นแนวทางในการปฏิบัติดังนี้

## ขั้นที่ 1 : เตรียมเครื่องเซิร์ฟเวอร์

เมื่อท่านจัดเตรียมเครื่องคอมพิวเตอร์เพื่อนำมาใช้งาน โดยการติดตั้งระบบปฏิบัติการสำหรับต่อเชื่อมกับอินเทอร์เน็ตเรียบร้อยแล้ว ท่านต้องติดตั้งซอฟต์แวร์สำหรับการทำเป็นเครื่องเว็บเซิร์ฟเวอร์ ซึ่งมีให้เลือกมากมายหลายยี่ห้อ ขึ้นอยู่กับว่าระบบปฏิบัติการของเครื่องเซิร์ฟเวอร์เป็นอะไร เช่น ถ้าท่านใช้ Windows NT อาจเลือก Microsoft IIS, Netscape Enterprise, Lotus Domino และอื่น ๆ แต่หากท่านเลือก Linux แล้ว อาจใช้ Apache สำหรับทำงานด้านการให้บริการเว็บเซิร์ฟเวอร์นี้ ซึ่งปัจจุบันเกือบทุกยี่ห้อรองรับการทำงานตามโปรโตคอล SSL และรองรับการติดตั้งหนังสือรับรองจากค่ายต่าง ๆ ด้วย

นอกจากนี้ท่านจะต้องเตรียมการเชื่อมต่อเข้าสู่อินเทอร์เน็ตเพื่อเปิดเว็บไซท์ของท่านสู่สาธารณะ

## ขั้นที่ 2 : เตรียมเอกสาร

การที่ท่านจะสร้างเว็บไซท์ให้น่าเชื่อถือโดยการมีหนังสือรับรองเว็บไซท์ได้ ท่านจะต้องดำเนินการขอหนังสือรับรองจากสถาบันผู้มีสิทธิออกหนังสือรับรอง ซึ่งสถาบันผู้ออกหนังสือเหล่านั้นจะตรวจสอบว่าท่านเป็นเจ้าของชื่อโดเมนที่จะจัดตั้งขายสินค้า และมีชื่อบริษัท ที่อยู่ และเอกสารอื่น ๆ ครบถ้วนถูกต้องหรือไม่ ซึ่งเอกสารที่สถาบันแต่ละแห่งต้องการอาจแตกต่างกันไปในแต่ละที่ เช่น ที่ บริษัท Thawte กำหนดให้ผู้ขอหนังสือรับรองส่งเอกสารประกอบการขอ 2 อย่าง คือ

1. หนังสือรับรองบริษัทหรือองค์กร
2. รายละเอียดยืนยันความเป็นเจ้าของชื่อโดเมนที่ต้องการจะนำหนังสือรับรองนี้ไปใช้ คือนำเอาต์พุตจากการใช้คำสั่ง whois แล้วตามด้วยชื่อโดเมนของท่าน เอาต์พุตนี้จะแสดงรายละเอียดเจ้าของชื่อโดเมน รวมทั้งองค์กรที่จดทะเบียนชื่อโดเมนของท่านด้วย

หากท่านสนใจจะขอหนังสือรับรองจากสถาบันใด กรุณาตรวจสอบเสียก่อนว่า สถาบันนั้น ๆ ต้องการเอกสารประกอบอะไรบ้างและเตรียมให้พร้อม (เอกสารทุกชิ้นต้องเป็นภาษาอังกฤษ)

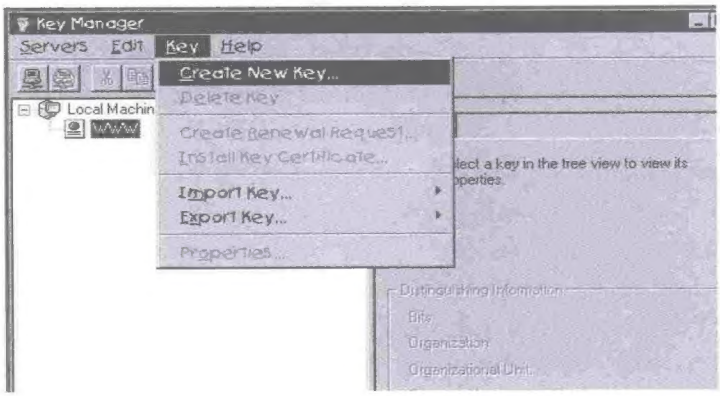
## ขั้นที่ 3 : สร้างคำร้องขอมีกุญแจ (Certificate Signing Request : CSR)

CSR จะต้องถูกสร้างจากเครื่องเว็บเซิร์ฟเวอร์ของท่าน โดยซอฟต์แวร์ที่ท่านใช้ทำงานด้านการให้บริการเว็บเซิร์ฟเวอร์จะต้องมีออปชันด้านการสร้างกุญแจสำหรับการเข้ารหัส เพื่อนำกุญแจที่ได้ไปใช้ในการขอหนังสือรับรอง

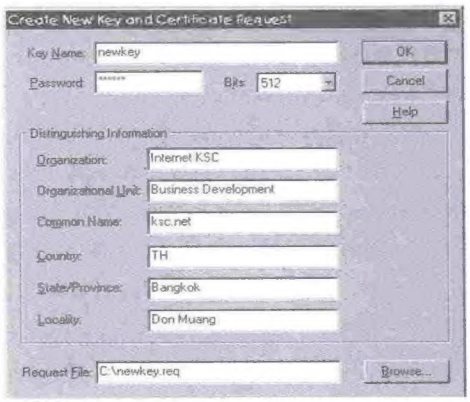
**ตัวอย่างการสร้างกุญแจใน Windows NT 4.0**

- ถ้าท่านติดตั้ง Microsoft Internet Information Server (IIS) แล้ว ใน Toolbar เลือก Microsoft Internet Server แล้วเลือก Key Manager เมื่อโปรแกรมถูกเปิดขึ้นมา ให้เลือก "WWW" แล้วไปที่เมนู Key เลือก "Create New Key..." ดังรูปที่ 1

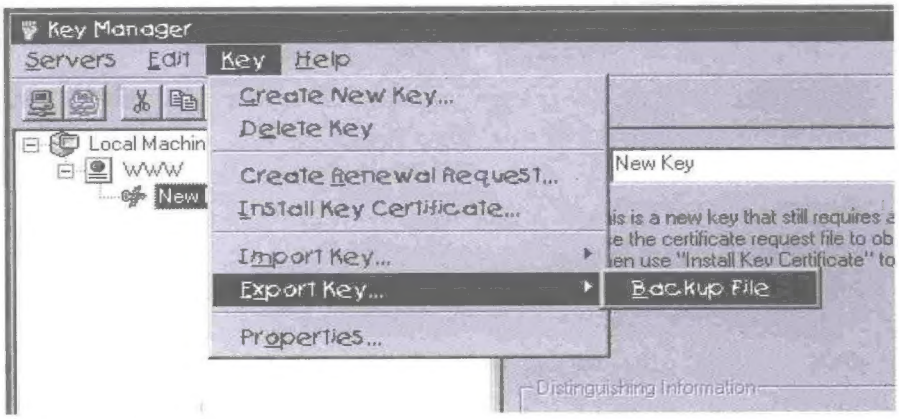
# Web Security : ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce




*รูปที่ 1 เลือกเมนูเพื่อสร้างกุญแจเข้ารหัส*




*รูปที่ 2 กรอกรายละเอียดสำหรับไฟล์ CSR*




*รูปที่ 3 การสำรองไฟล์ CSR*

● กรอกรายละเอียดและ Password แล้วเลือกว่าจะเก็บไฟล์ CSR นี้ที่ไหน ดังรูปที่ 2 เมื่อคลิก OK แล้ว จะมีการให้ยืนยัน Password อีกรอบ

* เพื่อเป็นการไม่ประมาท กรุณาทำสำรองไฟล์ที่ได้นี้อีกชุด เนื่องจากไฟล์นี้ยังเป็นไฟล์กุญแจสำหรับถอดรหัสอีกด้วย หากไฟล์สูญหาย ข้อมูลต่าง ๆ จะไม่สามารถถูกถอดรหัสได้ การสำรองโดยการ Backup ก็เพียงคลิกที่กุญแจที่สร้างไว้ แล้วเลือกเมนู Key, Export Key..., Backup File ดังรูปที่ 3

### ขั้นที่ 4 : ขอใบรับรอง

เมื่อได้ไฟล์ CSR ตามขั้นที่ 3 แล้ว ต้องนำรายละเอียดที่เขียนไว้ในไฟล์ไปใส่ในแบบฟอร์มการขอมีหนังสือรับรอง ซึ่งท่านจะต้องเข้าไปยังโฮมเพจของสถาบันผู้ออกหนังสือ (กรุณาดูกรอบแยกรายชื่อสถาบันผู้ออกหนังสือรับรองสำหรับใช้ SSL)

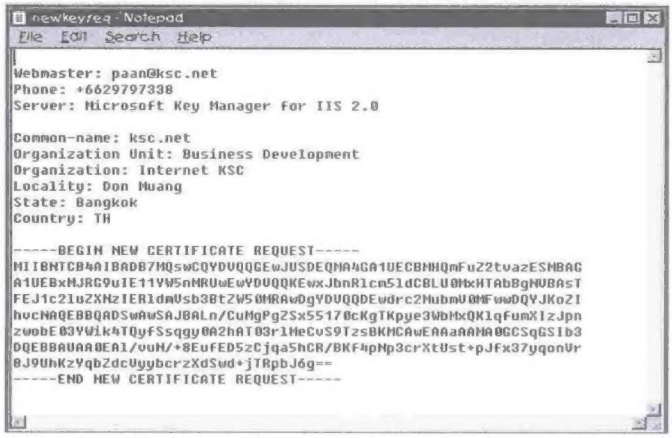
บนโฮมเพจของแต่ละสถาบันจะเปิดให้ท่านสมัครเพื่อขอหนังสือรับรอง โดยท่านจะต้องกรอกข้อมูลขององค์กร และต้องอ่านข้อกำหนดด้านกฎหมายให้เข้าใจก่อน และในส่วนสำคัญของการสมัคร ผู้สมัครจะต้องใส่ CSR ลงบนแบบฟอร์มในโฮมเพจนั้นด้วย เพื่อให้นำ CSR ไปสร้างหนังสือรับรองอีกที

### รายชื่อสถาบันผู้ออกหนังสือรับรองสำหรับใช้ SSL

สถาบันที่รับออกหนังสือรับรองเพื่อใช้กับโปรโตคอล SSL มีหลายแห่ง และราคาแตกต่างกันออกไป ท่านจะต้องเลือกดูว่าสถาบันที่ท่านสนใจมีหนังสือรับรองที่สามารถติดตั้งบนระบบปฏิบัติการของเซิร์ฟเวอร์ของท่านได้หรือไม่ เยี่ยมชมรายละเอียดได้ที่

- Verisign : www.verisign.com
- Thawte Consulting : www.thawte.com
- CertiSign Certificadora Digital Ltda. : www.certisign.com.br
- IKS GmbH : www.iks-jena.de
- BelSign NV/SA : www.belsign.de
- TC TrustCenter : www.trustcenter.de
- NLsign B.V. : www.nlsign.nl
- Deutsches Forschungsnetz : www.pca.dfn.de
- 128i Ltd. (New Zealand) : www.128i.com
- Entrust.net Ltd. : www.entrust.net
- Equifax Inc. : www.equifaxsecure.com
- GlobalSign NV/SA : www.globalsign.net

# Web Security : ขั้นตอนการสร้างความปลอดภัย สำหรับ E-Commerce




รูปที่ 4 ไฟล์ newkey.req

รูปที่ 5 คัดลอก CSR ของคุณมาใส่ในฟอร์มบนเว็บเพจ

**การใส่ CSR ทำได้โดย**

● เปิดไฟล์ CSR ที่ท่านสร้างและเก็บไว้ เช่น newkey.req ด้วยโปรแกรม Notepad ดังรูปที่ 4 ซึ่งท่านจะต้องคัดลอก CSR คือตั้งแต่คำว่า "——BEGIN NEW CERTIFICATE REQUEST——" ถึงคำว่า "——END NEW CERTIFICATE REQUEST——" ดังนั้น CSR ก็คือส่วนท้ายของไฟล์ CSR นั่นเอง ซึ่งจะมีหน้าตาดังนี้

```
——BEGIN NEW CERTIFICATE REQUEST——
MIIBNTCB4AIBADB7MQswCQYDVQQGEwJUSDEQMA4GA1
UECBMHQmFuZ2tvazESMBAGA1UEBxMJRG9uIE11YW5n
MRUwEwYDVQQKEwxJbnRlcm5ldCBLU0MxHTAbBgNVBAs
TFEJ1c2luZXNzIERldmVsb3BtZW50MRAwDgYDVQQDEwdrc
2MubmV0MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALn/
CuMgPgZSx55170cKgTKpye3WbMxQKlqfumXlzJpnzwobE03YWik4
TQyfSsqgy0A2hAT03rlMeCvS9TzsBKMCAwEAAaAAMA0GCSq
GSIb3DQEBBAUAA0EAI/vuN/+8EufED5zCjqa5hCR/
BKf4pNp3crXtUst+pJfx37yqonVr8J9UhKzYqbZdcVyybcrzXd
Swd+jTRpbJ6g==
——END NEW CERTIFICATE REQUEST——
```

* สำหรับซอฟต์แวร์เว็บเซิร์ฟเวอร์รุ่นเก่า CSR ที่ได้อาจจะหน้าตาไม่เหมือนตัวอย่างข้างต้นนี้นัก แต่ก็ใช้ได้เหมือนกัน

● นำส่วนที่คัดลอกไว้ไปใส่ในช่องของแบบฟอร์มในหน้าเว็บเพจ เช่น ที่ Thawte จะมีช่องสำหรับให้ใส่ CSR ดังรูปที่ 5

จากนั้นให้ส่งเอกสารประกอบการสมัครที่เตรียมไว้ทางแฟกซ์และส่งเอกสารตัวจริงตามไปโดยทางไปรษณีย์ตามที่อยู่ที่สถาบันกำหนด

หลังจากกรอกรายละเอียดด้านการชำระเงิน ก็เป็นอันเสร็จสิ้นขั้นตอนการสมัคร จากนี้ท่านจะต้องรอสถาบันที่ท่านสมัครไว้นี้ติดต่อส่งหนังสือรับรองไปให้

**ขั้นที่ 5 : ติดตั้งใบรับรองลงบนเซิร์ฟเวอร์**

หนังสือรับรองจะถูกส่งมาในรูปแบบไฟล์ ท่านจะต้องเก็บรักษาไฟล์ที่ได้เป็นอย่างดี และนำไฟล์นั้นมาติดตั้งลงบนเว็บเซิร์ฟเวอร์ ซึ่งไฟล์หนังสือรับรองจะมีหน้าตาดังนี้

```
——BEGIN CERTIFICATE——

JIEBSDSCEXoCHQEwLQMJSoZILvoNVQECSQAwcSETMRk
OAMUTBhMuVrMmIoAnBdNVBAoTF1JTQSBEYXRhIFNlY3
VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENlcn
RpZmljYXRlMSQwIgYDVQQDExtPcGVuIE1hcmtldCBUZXN0IFN
lcnZlciAxMTAwHhcNOTUwNzE5MjAyNzMwWhcNOTYwNTE0
MjAyOTEwWjBzMQswCQYDVQQGEwJVUzEgMB4GA1UECh
MXUlNBIERhdGEgU2VjdXJpdHksIEluYy4xHDAaBgNVBAsTE1Blcn
NvbmEgQ2VydGlmaWNhdGUxJDAiBgNVBAMTG09wZW4gTW
Fya2V0IFRlc3QgU2VydmVyIDExMDBcMA0GCSqGSIb3DQEBA
QUAA0sAMEgCQQDU7IrgR6vkVNX40BAq1poGdSmGkD1iN3sEPf
STGxNJXY58XH3JoZ4nrF7mIfvpghNi1taYimvhbBPNqYe4y
LPAgMBAAEwDQYJKoZIhvcNAQECBQADQQBqyCpws9
EaAjKKAefuNP+z+8NY8khckgyHN2LLpfhv+iP8m+bF66HNDUlFz
8ZrVOu3WQapgLPV90kIskNKXX3a

——END CERTIFICATE——
```

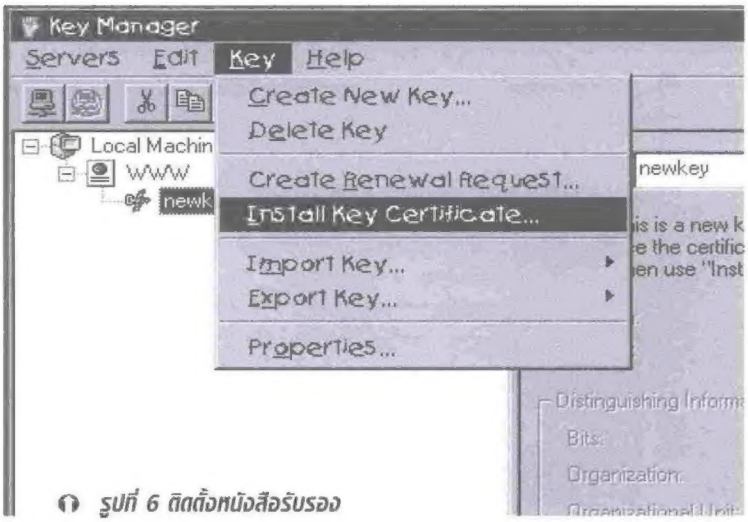
**การติดตั้งไฟล์หนังสือรับรอง** มีขั้นตอนคือ

● ใน Key Manager คลิกไปที่กุญแจที่สร้างไว้ แล้วไปที่เมนู Key เลือก "Install Key Certificate..." ดังรูปที่ 6

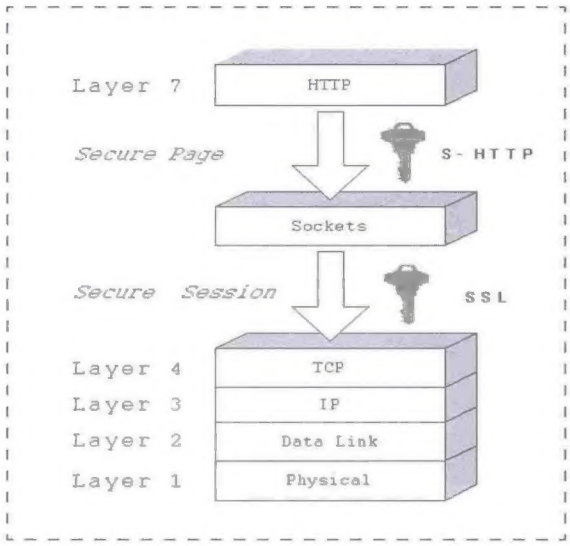
● เลือกไฟล์หนังสือรับรองที่เก็บไว้ และใส่ Password ที่กำหนดไว้ตอนสร้างไฟล์ CSR เพื่อยืนยันอีกรอบ

ส่วนการนำ SSL เข้าไปใช้ในไดเรคทอรีที่ต้องการ ทำได้โดย

● เลือก Internet Service Manager ใน Toolbar จากนั้นดับเบิลคลิกที่ "WWW" เพื่อแสดงหน้า Properties




รูปที่ 6 ติดตั้งหนังสือรับรอง




รูปที่ 7 เปรียบเทียบการทำงาน SSL กับ S-HTTP

● เลือก tab Directories เลือกไดเรคทอรีที่ต้องการ แล้วคลิก "Edit Properties"

● ในช่อง "Access" ให้เลือก "Require Secure SSL Channel"

เพียงเท่านี้เว็บเซิร์ฟเวอร์ของท่านก็สามารถใช้งาน SSL ได้แล้ว ซึ่งหากท่านใช้ซอฟต์แวร์เว็บเซิร์ฟเวอร์ยี่ห้ออื่น ๆ ท่านอาจต้องศึกษาขั้นตอนการสร้างไฟล์ CSR และการติดตั้งหนังสือรับรองจากคู่มือซอฟต์แวร์ของท่าน

## S-HTTP : Secure Hypertext Transfer Protocol

โปรโตคอล S-HTTP เป็นการเพิ่มส่วนการรักษาความปลอดภัยให้ HTTP ซึ่งเป็นโปรโตคอลสำหรับการส่งข้อมูลของ World Wide Web ซึ่ง S-HTTP ถูกพัฒนาตั้งแต่ปี 2537 โดย Enterprise Integration Technologies หรือ EIT โดยมุ่งหวังให้ S-HTTP เป็นตัวอย่างการนำเอาการเข้ารหัสที่ RSA พัฒนามาประยุกต์เข้ากับโปรโตคอลแอพพลิเคชัน ซึ่งได้เลือกเอา HTTP มาขยายส่วนการเข้ารหัส เนื่องจาก HTTP เป็นโปรโตคอลที่ใช้กันทั่วไป แต่ยังไม่มีส่วนการทำหน้าที่ดูแลความปลอดภัย

S-HTTP ต่างจาก SSL โดยสิ้นเชิง ดังรูปที่ 7 จากที่ได้กล่าวไปแล้ว S-HTTP เป็นการเพิ่มความปลอดภัยให้กับ HTTP โดยใส่กลไกการเข้ารหัสของข้อมูลในแพ็กเกตของ HTTP บนชั้น Application ในขณะที่ SSL ทำงานบนชั้น Transport ซึ่งจะดูแลด้านความปลอดภัยสำหรับช่องทางระหว่างโปรโตคอลชั้น Transport กับชั้น Application ดังนั้น SSL สามารถทำงานได้กับแอพพลิเคชันอื่น ๆ ที่ใช้โปรโตคอลจากชั้น Application ได้ ในขณะที่ S-HTTP เน้นเฉพาะโปรโตคอล HTTP และความแตกต่างอีกประการก็คือ SSL จะเข้ารหัสช่องทางการติดต่อระหว่างไคลเอนต์กับเซิร์ฟเวอร์ทั้งช่องในการติดต่อแต่ละครั้ง แต่ S-HTTP เข้ารหัสข้อความทีละข้อความ

หากท่านสนใจจะเปิดใช้ S-HTTP ลงบนเครื่องเซิร์ฟเวอร์ของท่าน สามารถเยี่ยมชมโปรแกรมเครื่องมือเพื่อช่วยให้ท่านสามารถนำ S-HTTP มาใช้ในการส่งข้อมูลได้ที่ http://www.terisa.com ซึ่งเป็นโฮมเพจของ Terisa Systems (เป็นบริษัทซึ่งก่อตั้งโดยความร่วมมือของ RSA Data Security และ EIT) โดยภายในโฮมเพจจะมีรายละเอียดผลิตภัณฑ์สำหรับนักพัฒนาเว็บ ได้แก่ ผลิตภัณฑ์ชื่อ DeviceSSL และ TLS Gold (ให้ท่านใช้โปรโตคอล TLS ได้ด้วย) เพื่อช่วยให้นักพัฒนานำทั้ง SSL และ S-HTTP เข้ามาเพิ่มความปลอดภัยทั้งกับหน้าเว็บเพื่องาน E-Commerce และการสร้างแอพพลิเคชันอื่น ๆ ได้อย่างสะดวก ผลิตภัณฑ์ของ Terisa นี้รองรับการเข้ารหัสทั้งแบบตามมาตรฐาน RSA และแบบใช้อัลกอริธึมอื่น ๆ ด้วย

อย่างไรก็ดี S-HTTP จะช่วยให้การส่งข้อมูลความลับสำหรับการทำ E-Commerce ปลอดภัยเช่นเดียวกับ SSL ท่านสามารถติดตั้งให้เครื่องเซิร์ฟเวอร์ของท่านมีการรักษาความปลอดภัยโดยใช้ทั้ง 2 โปรโตคอลในเวลาเดียวกันก็ได้ ยิ่งป้องกันมากยิ่งปลอดภัย แต่ท่านอาจประสบปัญหาด้านความเร็วในการทำงานได้ เนื่องจากทั้ง 2 โปรโตคอลต้องมีการเข้ารหัสข้อมูลซึ่งอาจทำให้การติดต่อรับส่งข้อมูลช้าลงได้

# Web Security : ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce

## SET : Secure Electronic Transaction

เมื่อปี 2539 ผู้นำด้านการให้บริการบัตรเครดิต 2 ราย คือ วีซ่า และมาสเตอร์การ์ด ร่วมมือกันสร้างมาตรฐานสำหรับการชำระเงินตัดบัตรเครดิตแบบ on-line ขึ้น โดยเน้นที่ความปลอดภัยและการให้ความมั่นใจทั้งผู้จ่ายและผู้รับเงินว่า ธุรกรรมแต่ละธุรกรรมที่ทำผ่านเครือข่ายจะได้รับการคุ้มครองและมีหลักประกันที่มั่นคง แต่ SET เป็นรูปแบบการชำระเงินที่ค่อนข้างซับซ้อนและต้องการโปรแกรมประกอบมากกว่า SSL เนื่องจาก SET ถูกออกแบบขึ้นมาเพื่ออุดช่องโหว่และข้อบกพร่องของ SSL

การชำระเงินแบบ SET จะต้องมีการตรวจสอบกันและกัน โดยผู้ขายจะต้องตรวจว่าบัตรเครดิตที่ผู้ซื้อใช้ชำระเงิน เป็นบัตรที่ใช้งานได้จริง มียอดเงินคงเหลือเพียงพอ ในขณะที่ฝ่ายผู้ซื้อก็ต้องตรวจสอบว่า ผู้ขายเป็นผู้ที่ไว้ใจได้ ไม่นำบัตรเครดิตของตนไปใช้ในทางที่ไม่ควร ดังนั้น SET จึงใช้วิธีแต่งตั้งบุคคลที่ 3 เป็นผู้ออกใบรับรองทั้ง 2 ฝ่าย รวมทั้งวิธีการป้องกันกรณีผู้ขายแอบนำหมายเลขบัตรเครดิตที่ได้มาไปใช้โดยไม่ได้รับอนุญาตอีกด้วย ซึ่งอาจสรุปได้ว่า SET จะต้องมีผู้ร่วมทำธุรกรรมทั้งหมด 4 ฝ่าย และแต่ละฝ่ายมีโปรแกรมสำหรับทำหน้าที่ของตนดังต่อไปนี้

**1. ผู้ซื้อ กับ โปรแกรมกระเป๋าสตางค์** : โปรแกรมกระเป๋าสตางค์ หรือ e-Wallet เป็นโปรแกรมไคลเอนต์ที่ใช้ติดต่อกับโปรแกรมทางฝั่งเซิร์ฟเวอร์โดยอัตโนมัติ เพื่อตรวจสอบว่าเซิร์ฟเวอร์ที่ต้องการสั่งซื้อสินค้านี้มีใบรับรองว่าเป็นตัวตนจริง ๆ หรือไม่ รวมทั้งโปรแกรม e-Wallet จะตรวจสอบว่าเซิร์ฟเวอร์นี้มีการติดต่อกับสถาบันการเงินที่ไหน เป็นสถาบันที่มีใบรับรองหรือไม่

**2. ผู้ขาย กับ โปรแกรมฝ่ายขาย** : โปรแกรมฝ่ายขาย หรือ Merchant Server เป็นโปรแกรมที่รวมเอาเทคโนโลยีด้านความปลอดภัยของข้อมูลเข้าไว้ด้วยกัน เนื่องจาก Merchant Server นี้จะต้องติดต่อกับทั้งผู้ซื้อและสถาบันการเงินของผู้ซื้อ รวมทั้ง Merchant Server จะควบคุมการแลกเปลี่ยนและตรวจสอบใบรับรองก่อนที่จะมีการซื้อขายอีกด้วย

**3. ธนาคาร กับ โปรแกรมการชำระเงิน** : โปรแกรมชำระเงิน หรือ Payment Gateway Server นี้จะช่วยให้ธนาคารสามารถดำเนินการรับชำระเงินจากผู้ซื้อได้ Payment Gateway Server ช่วยเชื่อมผู้ซื้อและผู้ขายในการซื้อขายเข้ากับระบบการชำระเงิน เพื่อให้การซื้อขายนั้นสำเร็จลุล่วง

## ใบรับรองตามมาตรฐาน SET

เนื่องจาก SET ถูกสร้างขึ้นตามหลักการการใช้ใบรับรองดิจิตอลมาตรฐาน X.509 เวอร์ชัน 3 ดังนั้นการติดต่อระหว่างทุก ๆ ฝ่าย จึงจะต้องมีการอ้างอิงใบรับรองของตัวเองและตรวจสอบใบรับรองของฝ่ายตรงข้าม เพื่อความมั่นใจในการติดต่อ ใบรับรองของโปรโตคอล SET นี้จะไม่เหมือนใบรับรองทั่วไป เนื่องจากใบรับรองของ SET จะต้องใช้กับโปรแกรมส่วนอื่น ๆ ที่เป็นองค์ประกอบของการชำระเงินแบบ SET ได้แก่ โปรแกรม e-Wallet, โปรแกรม Merchant และโปรแกรม Payment Gateway

**ใบรับรองมาตรฐาน SET แบ่งเป็น 3 ประเภท**

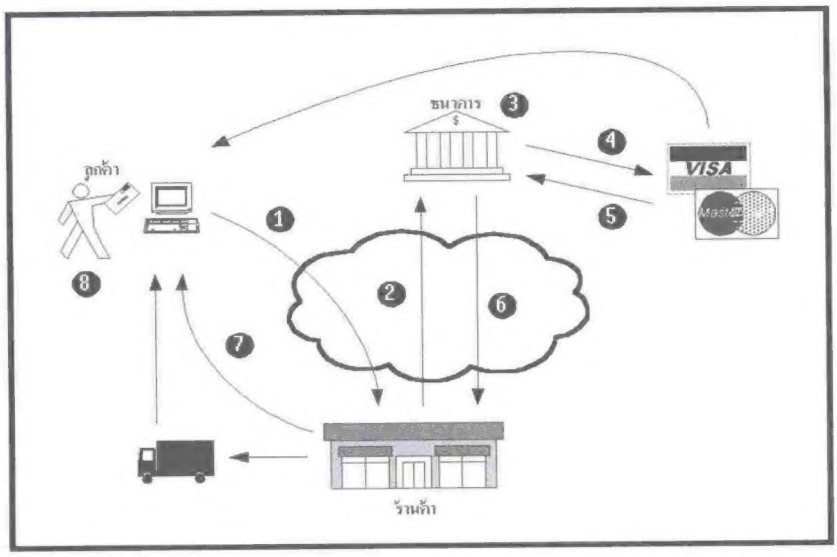
**1. ใบรับรองผู้ซื้อ (Card-Holder Certificate)** เป็นตัวแทนบัตรเครดิต/เดบิตในรูปแบบอิเล็กทรอนิกส์สำหรับให้ผู้ถือบัตรนั้นใช้จ่าย รายละเอียดของบัตร ไม่ว่าจะเป็นหมายเลขบัตร วันหมดอายุ และสถาบันผู้ออกบัตร จะถูกเข้ารหัสไว้หมด และไม่สามารถนำมาแกะดูรายละเอียดเหล่านั้นได้ แม้ว่าจะได้ใบรับรองนี้ไปแล้ว เนื่องจากใบรับรองเหล่านี้ถูกเข้ารหัสไว้ Card-Holder Certificate จะต้องนำไปติดตั้งเข้ากับโปรแกรม e-Wallet ในเครื่องของผู้ซื้อ เพื่อใช้ซื้อสินค้า

**2. ใบรับรองผู้ขาย (Merchant Certificate)** ผู้ขายแต่ละรายอาจมีใบรับรองหลายใบจากสถาบันผู้ออกบัตรเครดิตหลายแห่ง หมายความว่า หากผู้ซื้อใช้บัตรเครดิตยี่ห้อ A ผู้ขายก็จะต้องมีใบรับรองสำหรับการรับบัตรยี่ห้อ A นี้ด้วย เพื่อใช้เป็นคู่กันกับผู้ซื้อในการซื้อขาย Merchant Certificate ประกอบด้วย ได้แก่ รายละเอียดของผู้ขาย กุญแจสาธารณะของผู้ขาย และกุญแจสาธารณะของธนาคารที่ผู้ขายมีบัญชีอยู่

**3. ใบรับรองผู้ชำระเงิน (Payment Gateway Certificate)** หากธนาคารของผู้ขายติดตั้งโปรแกรม Payment Gateway เพื่อรับชำระเงินแทนผู้ขายแล้ว จะต้องมี Payment Gateway Certificate ด้วยเพื่อยืนยันว่าธนาคารนี้มีสิทธิเป็นผู้รับเงิน และมีสิทธิเป็นผู้สอบถามยอดบัญชีบัตรเครดิตของผู้ซื้อ ก่อนจะตัดบัตรตามราคาสินค้าที่ผู้ซื้อสั่งซื้อ

ในการทำ Transaction แบบ SET นี้จะต้องมีการตรวจสอบใบรับรองกันและกันเสมอ ซึ่งเป็นการยืนยันความปลอดภัย และป้องกันความผิดพลาดกรณีที่มีผู้แอบอ้างหมายเลขบัตรเครดิตได้อีกด้วย

## Web Security : ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce




รูปที่ 8 ขั้นตอนการชำระเงินตามโปรโตคอล SET

รูปที่ 9 เครื่องหมาย SET

**4. สถาบันผู้ออกบัตรเครดิตให้ผู้ซื้อ กับ โปรแกรมออกใบรับรอง :** โปรแกรมออกใบรับรอง หรือ Certificate Authority เมื่อผู้ซื้อที่ถือบัตรเครดิตต้องการซื้อสินค้าด้วยโปรโคตอล SET นี้ จะต้องติดต่อสถาบันผู้ออกบัตรเครดิตของตนให้ออกใบรับรอง หรือ Certificate ที่เป็นมาตรฐานตามโปรโตคอล SET (เป็นคนละอย่างกับใบรับรองแบบ SSL นะคะ กรุณาอ่านกรอบย่อย ใบรับรอง SET ประกอบ) ซึ่งโปรแกรม Certificate Authority นี้จะช่วยให้สถาบันการเงินเหล่านั้นใช้ออกใบรับรองดิจิตอลให้กับผู้ถือบัตรเครดิตและบรรดาร้านค้า เพื่อเป็นมาตรฐานในการตรวจสอบกันและกันระหว่างผู้ซื้อกับผู้ขาย

ขั้นตอนการทำ Transaction ตามโปรโตคอล SET ดังรูปที่ 8

1. เมื่อผู้ซื้อเลือกสินค้าที่ต้องการได้แล้ว ก็จะยืนยันว่าพร้อมชำระเงิน โดยการคลิกที่หน้าเว็บแสดงสินค้านั้น โปรแกรม e-Wallet ซึ่งติดตั้งพร้อมใบรับรองผู้ซื้อบนเครื่องคอมพิวเตอร์ที่ผู้ซื้อใช้อยู่นั้นจะถูกเปิดขึ้นเพื่อให้ผู้ซื้อเลือกบัตรเครดิตที่ต้องการใช้ (กรณีผู้ซื้อถือบัตรหลายใบ) เมื่อผู้ซื้อเลือกบัตรที่ต้องการแล้ว โปรแกรม e-Wallet จะจัดการนำหมายเลขบัตรเครดิตเข้ารหัสด้วยกุญแจสาธารณะของธนาคารที่ได้มา แล้วส่งไปยังเครื่องเว็บเซิร์ฟเวอร์ของผู้ขาย

2. โปรแกรม Merchant ได้รับรายละเอียดดังกล่าว ก็จะส่งต่อไปยังธนาคารที่ผู้ขายมีบัญชีอยู่ เพื่อให้ธนาคารรับการจ่ายเงินจากผู้ซื้อ เนื่องจากโปรแกรม Merchant นี้ไม่สามารถถอดรหัสหมายเลขบัตรเครดิตได้

3. โปรแกรม Payment Gateway ที่ติดตั้งที่ธนาคารได้รับรายละเอียดจากที่ Merchant ส่งผ่านมา จะทำการถอดรหัสจนได้หมายเลขบัตรเครดิตที่ผู้ซื้อต้องการใช้ชำระเงิน

4. Payment Gateway ส่งต่อหมายเลขบัตรเครดิตให้สถาบันผู้ออกบัตรตรวจสอบว่าบัตรนี้ใช้ชำระเงินได้ตามจำนวนที่สั่งซื้อหรือไม่ แน่นอนว่าจะต้องเข้ารหัสข้อมูลก่อนส่งด้วยกุญแจสาธารณะของสถาบันผู้ออกบัตร

5. สถาบันผู้ออกบัตรอนุมัติการชำระเงินผ่านบัตรตามหมายเลขที่ได้ พร้อมทั้งหักยอดเงินในบัญชีบัตรเครดิตของผู้ซื้อตามจำนวนที่ได้สั่งซื้อ จากนั้นส่งคำยืนยันการอนุมัติกลับไปยังธนาคาร

6. ธนาคารนำฝากเงินใส่ในบัญชีของผู้ขายตามจำนวนที่ขายสินค้าได้ และตอบยืนยันกลับไปยังโปรแกรม Merchant ว่าได้รับชำระเงินเรียบร้อยแล้ว

7. Merchant ยืนยันการขายให้โปรแกรม e-Wallet

8. สิ้นเดือนผู้ซื้อจะได้รับใบแจ้งหนี้บัตรเครดิตที่ได้สั่งซื้อไปแล้ว

ปัจจุบันมีผลิตภัณฑ์ยี่ห้อต่าง ๆ ที่พัฒนาขึ้นมาตามโปรโตคอล SET ซึ่งคณะกรรมการทำงานและพัฒนา SET ได้กำหนดให้ผลิตภัณฑ์เหล่านั้นต้องผ่านการทดสอบตามมาตรฐานของโปรโตคอล เพื่อให้การทำธุรกรรมร่วมกันได้ นั่นคือ หากผู้ซื้อ ผู้ขาย ธนาคาร และสถาบันผู้ออกบัตร ใช้ผลิตภัณฑ์ต่างยี่ห้อกัน ก็สามารถทำการซื้อขายได้

ร้านค้าที่ติดตั้งโปรแกรม Merchant และได้รับใบรับรองผู้ขาย (Merchant Certificate) เพื่อติดต่อกับธนาคารและสถาบันผู้ออกบัตรเครดิตสำหรับการซื้อขายสินค้าตามมาตรฐาน SET จะได้เครื่องหมาย SET ดังรูปที่ 9 เพื่อนำขึ้นไปแสดงบนหน้าเว็บอีกด้วย

*ผลิตภัณฑ์ที่ผ่านการทดสอบตามมาตรฐาน SET มีดังนี้*

**ประเภท : e Wallet**

| ชื่อผู้ผลิต | ชื่อผลิตภัณฑ์ | ระบบปฏิบัติการ |
|---|---|---|
| Brokat | X•PAY™ Java Credit Wallet 2.0 | Java Virtual Machine 1.1 |
| CyberCash | CyberCash Wallet 4.0 | Windows NT 4.x |
| Fujitsu | CommerceSTAGE™ Secure Credit Cardholder v2.0 | Windows NT<br>Windows 98<br>Windows 95 |
| Globeset | Globeset Server Wallet™ 1.2 | Windows NT 4.0<br>HP UX 10.20,<br>Solaris 2.5 |
| Hitachi | Cardholder Wallet Product 01-04 | Windows 9x, Windows NT 4.0 |
| IBM | IBM Consumer Wallet™ 2.1 | Windows NT 4.0<br>Windows 9x |
| Samsung | Wallet 1.0 | Windows 9x |
| Trintech | S/PAY 2.1 | Windows NT 4.0<br>Windows 9x |
| VeriFone | vWALLET™ 2.1 | Windows NT 4.0<br>Windows 9x |

**ประเภท : Merchant Server**

| ชื่อผู้ผลิต | ชื่อผลิตภัณฑ์ | แพล็ตฟอร์ม |
|---|---|---|
| Brokat | X•PAY™ Server 2.0 | Windows NT, Sun Solaris 2.5.1 and 2.6, Linux suse 5.3 |
| CyberCash | CyberCash CashRegister 4.0 | Sun OS 5.6 |
| Fujitsu | CommerceSTAGE™ CyberShop Credit Payment v2.0 | Windows NT 4.0<br>Solaris 2.5 and 2.6 |
| Globeset | Globeset Server POS™ 1.4 | Windows NT 4.0<br>Solaris 2.5, 2.6<br>HP-UX 10.20 |
| Hitachi | Merchant Server Product 01-01 | Windows NT 4.0 |
| IBM | 1) IBM Payment Server™ 1.2<br>2) IBM Websphere Payment Manager 2.1 | 1) Windows NT 4.0, AIX 4.2 & 4.3, Solaris 2.5.1,OS390 1.3 & 2.4, OS400 V4R3;<br>2) Windows NT 4.0, AIX 4.2.1, 4.3.2 & 4.3.3, Solaris 2.6, OS390 2.7, OS400 V4R4 |
| ProfiTrade 90 Ltd | JavaMerchant with SET v1.0 | JDK 1.1 |
| Trintech | S/PAY 2.2.3 | Windows NT 4.0<br>Windows 9x |
| VeriFone | vPOS™ 4.5 | Windows NT 4.0 |

**ประเภท : Payment Gateway server**

| ชื่อผู้ผลิต | ชื่อผลิตภัณฑ์ | แพล็ตฟอร์ม |
|---|---|---|
| Brokat | X•PAY™ Gateway 2.0 | Windows NT 4.0, Sun Solaris 2.51 and 2.6 |
| Fujitsu | CommerceSTAGE™ Credit Payment Gateway v2.0 | Solaris 2.5 and 2.6 |
| Globeset | Globeset Gateway™ 1.4 | Windows NT 4.0<br>Solaris 2.5, 2.6 |
| Hitachi | Payment Gateway Product 01-01 | Windows NT 4.0 |
| IBM | IBM Payment Gateway™ 1.2 | AIX 4.2.1<br>S/390 |
| Oasis Technology Ltd. | Oasis Payment Gateway v1.0 | Solaris 2.7, HP_UX 11.0, AIX 4.3, Compaq OSF 4.0D |
| PrivyLink | PrivyGateway | Sun 5.5.1 |
| Trintech | S/PAY 2.5 | Windows NT 4.0<br>Windows 9x |
| VeriFone | vGATE™ 4.1 | HPUX 10.x |

| ประเภท : Certificate Authority | | |
|---|---|---|
| ชื่อผู้ผลิต | ชื่อผลิตภัณฑ์ | แพล็ตฟอร์ม |
| Fujitsu | CommerceSTAGE™ Secure Certificate Authority v2.0 | Solaris 2.5 and 2.6 |
| Globeset | Globeset CA™ 1.4 | Windows NT 4.0<br>Solaris 2.5, 2.6 |
| Hitachi | Certificate Authority 01-03 | HP-UX10.20 |
| IBM | IBM Payment Registry™ 1.2 | AIX 4.x |
| PrivyLink | PrivyTrust v1.0 | Sun OS 5.5.1 |
| VeriSign | Certificate Authority Services 1.1.0 | SUN OS 5.5.1 |

## หากต้องตัดสินใจ

จะเห็นได้ว่า SSL และ S-HTTP นั้นนำมาใช้งานได้ง่ายและประหยัด ท่านอาจต้องเสียค่าใช้จ่ายเฉพาะค่าจดทะเบียนหนังสือรับรองสำหรับร้านค้าเท่านั้น ส่วนผู้ซื้อก็สามารถใช้ SSL สำหรับซื้อขายได้โดยไม่ต้องเสียเงินค่าโปรแกรมและหนังสือรับรอง รวมทั้งไม่ต้องติดตั้งโปรแกรมเพิ่มเติมลงบนเครื่องคอมพิวเตอร์ก่อนทำการซื้ออีกด้วย แต่กระนั้น SSL และ S-HTTP ยังมีช่องโหว่อีกหลายประการ เช่น หากมีคนแอบนำหมายเลขบัตรเครดิตของคนอื่นมาใช้ ร้านค้าก็ไม่สามารถตรวจสอบได้เลย ทำให้ร้านค้าต้องรับความเสี่ยงหากเจ้าของบัตรปฏิเสธการจ่ายเงินนั้น

SET ช่วยอุดช่องโหว่เหล่านี้ เนื่องจาก SET มีระบบการตรวจสอบที่รัดกุม แต่ข้อเสียของ SET ก็คือ ความยุ่งยากในการสั่งซื้อ เนื่องจากผู้ซื้อต้องติดตั้งโปรแกรมเพิ่มเติม และปัญหาที่สำคัญคือ ค่าใช้จ่าย เนื่องจากซอฟต์แวร์และหนังสือรับรองตามโปรโตคอล SET มีราคาสูงมาก

อย่างไรก็ตาม มีการคาดการณ์กันว่า SSL จะยังเป็นโปรโตคอลสำหรับการทำ E-Commerce ที่แพร่หลายที่สุดในระยะเวลา 3 ปีนี้ ซึ่งถึงเวลานั้น ราคาของ SET อาจลดลงมาจนเป็นมาตรฐานใหม่ที่ทุกคนต้องใช้ก็ได้ แต่ก่อนจะถึงเวลานั้น SSL ก็ได้มีการปรับปรุงและพัฒนาขึ้นเรื่อย ๆ โดยเมื่อเดือนกรกฎาคม 2541 Netscape Communications ได้มอบสิทธิความเป็นเจ้าของโปรโตคอล SSL ให้กับ Internet Engineering Task Force (IETF) ซึ่งเป็นหน่วยงานกลาง ทำงานด้านความปลอดภัยทางอินเทอร์เน็ต ซึ่ง IETF ได้ปรับปรุง SSL และเปลี่ยนชื่อเป็น Transport Layer Security (TLS) TLS นี้จะถูกปรับแต่งให้มีออปชันเสริมด้านการตรวจสอบว่าผู้ที่ติดต่อด้วยเป็นตัวตนจริง ๆ กับที่อ้างไว้หรือไม่ ซึ่งการตรวจสอบนี้จะใช้การตรวจหนังสือรับรองตามมาตรฐาน X.509 ซึ่งเราก็ต้องจับตาดูกันต่อไปว่า TLS จะมาเป็นคู่แข่ง SET หรือไม่

หากท่านอ่านบทความนี้จนจบ และเริ่มเกิดไอเดียแล้วว่า จะเพิ่มความปลอดภัยให้กับการซื้อขายได้อย่างไรแล้วนั้น สิ่งหนึ่งที่ท่านจะต้องตระหนักก็คือ ข้อมูลรายละเอียดลูกค้า ไม่ว่าจะเป็น สินค้าที่ลูกค้าเลือกซื้อ ที่อยู่ และลักษณะการชำระเงินของลูกค้า เป็นข้อมูลที่มีค่ามากกว่า หากผู้ขายนำข้อมูลเหล่านั้นไปใช้ในทางที่ไม่เหมาะสม หรือก่อให้เกิดการรบกวนลูกค้าเสียเอง ความปลอดภัยใด ๆ ก็ไม่มีความหมาย